REMARKS

Claim 13-15 have been canceled. Claims 1-12, 16, and 17 remain pending.

The Examiner has rejected claims 1-17 under 35 U.S.C. 102(e) as being anticipated by Porras et al.

The rejection is respectfully traversed. With respect to claim 1, Porras teaches consolidating alerts generated by another system or process. Porras describes (column 6, lines 5-12) how "by analogy, a single criminal intrusion into a physical property might trigger alarms on multiple sensors such as a door alarm and a motion detector, ... , but from an informational perspective both alarms are essentially signaling the same event." In contrast, claim 1 recites, "an analysis engine configured to identify backward and forward time steps in the logfile, correlate the time steps with events, and assign a suspicion value to an event." The specification describes (page 83 line 14 to page 87 line 5) how backward and forward time steps in a log file may be used detect intrusions. Porras does not describe an analysis engine configured to identify backward and forward time steps in the logfile, correlate the time steps with events, and assign a suspicion value to an event. As such, claim 1 is believed to be allowable.

Claims 2-12 depend from claim1 and are believed to be allowable for the same reasons described above.

Claims 13-15 have been canceled.

Like claim 1, claims 16 and 17 recite detecting intrusions on a host, including, "collecting information including events and timestamps from a logfile, identifying backward and forward time steps in the logfile, correlating the backward and forward time steps with events, and

assigning a suspicion value to an event." As such, claims 16 and 17 are believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 8/11/2004

Clover Huang

Clover Huang
Registration No. 55,285
V 408-973-2594
F 408-973-2595

VAN PELT AND YI, LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014